IN THE UNITED STATES DISTRICT COURT FOR THE MIDDLE DISTRICT OF TENNESSEE

THERAPY MY WAY and THOMAS FRANCO THERAPY AND CONSULTING, individually and on behalf of all others similarly situated, Plaintiffs, v. CHANGE HEALTHCARE INC., OPTUM, INC. and UNITEDHEALTH GROUP INCORPORATED, Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

TABLE OF CONTENTS

Plaintiffs Therapy My Way and Thomas Franco Therapy and Consulting ("Plaintiffs"), individually and on behalf of all others similarly situated, alleges the following:

I. INTRODUCTION

1. Plaintiffs bring this proposed class action lawsuit against Defendants Change Healthcare Inc., Optum, Inc. and UnitedHealth Group Incorporated ("Defendants") for their failure to maintain the security of their computer networks in accordance with state and federal law. Defendants' computer networks include data processing systems, portals, and platforms that have become critical infrastructure for administering healthcare across the United States. Defendants' computer networks process billions of healthcare transactions annually, performing more than 100 critical functions used by over 1,000,000 healthcare providers, including hospitals, physicians, therapists, pharmacies, and laboratories, and affecting medical care for many millions of Americans. Through aggressive acquisition and expansion, Defendants have broadened the reach of their services to include the systems that healthcare providers use to submit claims for payment to insurers and other payors, platforms that verify individuals' insurance coverage, programs used to verify prior authorizations for medical treatment and prescription drugs, and dozens of other critical functions.

2. Given their role providing critical infrastructure in the nationwide delivery of healthcare, Defendants knew they needed to implement incredibly robust cybersecurity controls to prevent disruptions. Lives are literally on the line. Instead, Defendants neglected to implement the robust cybersecurity controls that such critical infrastructure demands. As a result of Defendants' negligence, failures, and omissions, a well-known group of cybercriminals, called ALPHV/Blackcat ("Blackcat") that have been known for some time to target healthcare organizations, was able to infiltrate Defendants' computers networks and steal for ransom confidential health data and source code, among other things ("Data Breach").

3. The Data Breach exposed the vulnerabilities in Defendants' computer networks and as a result, Defendants took all of the affected computer networks offline, leaving healthcare providers in dire straits. Since the Data Breach was discovered on February 21, 2024, healthcare providers have been unable to provide critical services and get paid on claims for medical treatment

they have provided. Defendants' negligence, failures, and omissions have catastrophically harmed hard-working medical providers around the country, forcing many to the edge of bankruptcy and delaying or denying vital medical treatments needed by patients around the county.

4. The American Hospital Association ("AHA") has described the situation as a "staggering loss of revenue."[1] According to an estimate from First Health Advisory, a digital risk assurance firm, the Data Breach "is costing some providers over $100 million a day."[2] Rick Pollack, President and CEO of the AHA, remarked that the Data Breach is the "most serious incident of its kind leveled against a U.S. healthcare organization."

5. The healthcare industry has been a target of cyberattacks for years given the massive amount of confidential personal health information ("PHI") and personal identifying information ("PII") that healthcare organizations collect, store, and maintain and that can be used to commit identity theft. Since as early as 2014, government agencies have warned the healthcare industry about the threat of cyberattacks and has repeatedly cautioned them to ensure that their systems are secure and protected. The U.S. government has also specifically warned the industry that Blackhat has hit at least 70 organizations since December 2023, a majority of them healthcare organizations. Therefore, the Data Breach and related shutdown were entirely foreseeable and could have been avoided.

6. Plaintiffs, individually and on behalf of all others similarly situated, allege claims for negligence and for unjust enrichment.

II. PARTIES

7. Plaintiff Therapy My Way is a citizen of New York and maintains its principal place of business in Plainview, NY.

8. Plaintiff Thomas Franco Therapy and Consulting is a citizen of New York and maintains its principal place of business in Manhattan, NY.

---

[1] *See* https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack (last visited March 18, 2024).

[2] *Id.*

9. Defendant Change Healthcare Inc. is a publicly traded company with its principal place of business in Nashville, Tennessee and is incorporated in Delaware. It became a subsidiary of UnitedHealth Group Incorporated in 2022 and is operated by Optum, Inc., another UnitedHealth Group subsidiary.

10. Defendant Optum, Inc. maintains its principal place of business in Eden Prairie, Minnesota and is incorporated in Delaware.

11. Defendant UnitedHealth Group Incorporated is one of the largest publicly traded companies by revenue and maintains its principal place of business in Minnetonka, Minnesota and is incorporated in Delaware. UnitedHealth Group exercises control over the management of the Change Healthcare cybersecurity systems as evidenced by UnitedHealth Group's response to the Data Breach as alleged herein.

III. JURISDICTION AND VENUE

12. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of the individual class members exceed the sum or value of $5,000,000, exclusive of interests and costs, and this is a class action in which one or more members of the proposed Class, including Plaintiffs, are citizens of a state different from Defendants. The Court has supplemental jurisdiction over the alleged state law claims under 28 U.S.C. § 1367 because they form part of the same case or controversy.

13. This Court may exercise jurisdiction over Defendants because they are registered to conduct business in Tennessee; have sufficient minimum contacts in Tennessee; and intentionally avail themselves of the markets within Tennessee through the promotion, sale, and marketing of their services, thus rendering the exercise of jurisdiction by this Court proper and necessary.

14. Venue is proper in this District under 28 U.S.C. § 1391 because Defendant Change Healthcare Inc. resides in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Background

15. Change Healthcare is a healthcare technology company that works across the U.S. health system "to make clinical, administrative and financial processes simpler and more efficient for payers, providers, and consumers." Change Healthcare offers healthcare providers such as doctors, hospitals, therapists, pharmacies, laboratories, and clinics services and support in key areas such as provider claim processing, pharmacy claim transactions, verification of insurance, disbursement of provider payments, and authorizations and medical necessity reviews. Healthcare providers utilize Change Healthcare's services either through a direct contractual relationship or indirectly through third-party intermediaries.

16. According to the Change Healthcare website, its "extensive network, innovative technology, and expertise inspire a stronger, better coordinated, increasingly collaborative, and more efficient healthcare system." It bills itself as a "trusted partner for organizations committed to improving the healthcare system through technology."

17. Change Healthcare also represents to providers that its "advanced technology and services help . . . enhance patient engagement and access, improve outcomes, drive revenue performance, and improve operational efficiency." Change Healthcare represents to payers that its "advanced technology solutions and services help payers achieve their priorities across the member journey." Change Healthcare promises its partners that its "advanced technology solutions empower our partners to achieve their strategic business objectives and meet their customers' needs." And it assures patients that its "solutions streamline the engagement, care, and payment experience to improve the patient journey."

18. Change Healthcare processes 15 billion healthcare transactions annually and touches one in every three U.S. patient records through its clinical connectivity solutions.

19. Previously, Change Healthcare was an independent company that was not owned by any particular healthcare provider or insurer. In 2021, UnitedHealth Group ("UHG") proposed a deal to acquire Change Healthcare for a merger with Optum, a healthcare provider and subsidiary of UHG.

20. Melinda Reid Hatton, AHA Vice President and General Counsel, voiced concerns about the proposed deal and wrote to the Department of Justice ("DOJ") asking it to investigate. In the letter to the DOJ, Ms. Hatton wrote, "The proposed acquisition would produce a massive consolidation of competitively sensitive healthcare data and shift such data from Change Healthcare, a neutral third party, to Optum."[3]

21. The DOJ investigated and filed a complaint to stop UHG's transaction. In its complaint, the DOJ described Change Healthcare as a technology company that operates "the nation's largest electronic data interchange (EDI) clearinghouse, which transmits data between healthcare providers and insurers, allowing them to exchange insurance claims, remittances, and other healthcare-related transactions . . . It has access to a vast trove of competitively sensitive claims data that flows through its EDI clearinghouse—over a decade's worth of historic data as well as billions of new claims each year."[4]

22. Moreover, according to the DOJ, "50 percent of all medical claims in the United States pass through Change's EDI clearinghouse.[5] Change's self-described 'pervasive network connectivity,' including approximately '900,000 physicians, 118,000 dentists, 33,000 pharmacies, 5,500 hospitals and 600 laboratories,' means that even when United's health insurer rivals choose not to be a Change customer, health insurers have no choice but to have their claims data pass through Change's EDI clearinghouse. Not only does Change process vast amounts of competitively sensitive claims data, but it also has secured 'unfettered' rights to use over 60 percent of this data for its own business purposes including, for example, using claims data for healthcare

[3] *See* https://www.darkdaily.com/2021/04/07/aha-expresses-opposition-to-merger-between-unitedhealth-groups-optuminsight-and-change-healthcare-doj-agrees-to-look-into-the-13b-deal/ (last visited March 18, 2024).

[4] *See* https://www.justice.gov/atr/case-document/file/1476901/dl (last visited March 18, 2024).

[5] *Id.*

analytics. Additionally, through its claims editing product, Change has access to the proprietary plan and payment rules for all of United's most significant health insurance competitors."[6]

23. The DOJ, however, lost its challenge to UHG's acquisition of Change Healthcare after a district judge ruled in UHG's favor and the DOJ chose not to appeal.

24. In October 2022, Optum completed its combination with Change Healthcare. According to a press release UHG issued, "The combined businesses share a vision for achieving a simpler, more intelligent and adaptive health system for patients, payers and care providers. The combination will connect and simplify the core clinical, administrative and payment processes health care providers and payers depend on to serve patients. Increasing efficiency and reducing friction will benefit the entire health system, resulting in lower costs and a better experience for all stakeholders."[7]

B. The February 2024 Data Breach Exposed Significant Vulnerabilities in Defendants' Computer Networks, Leading to the Shutdown of Critical Healthcare Infrastructure.

25. On February 21, 2024, Defendants discovered the Data Breach and that their computer networks were not secure and could not protect PHI and PII as required by state and federal law. UHG set up a website regarding the Data Breach at www.unitedhealthgroup.com to announce the Data Breach and stated that it disconnected the Change Healthcare systems.[8] UHG made a similar statement in a filing with the U.S. Securities and Exchange Commission.[9] UHG also stated, "The Company has retained leading security experts, is working with law enforcement and notified customers, clients and certain government agencies . . . At this time,

---

[6] *Id.*

[7] *See* https://www.optum.com/en/about-us/news/page.hub.optum-and-change-healthcare-complete-combination.html (last visited March 18, 2024).

[8] *See* https://www.unitedhealthgroup.com/newsroom/2024/2024-03-07-uhg-update-change-healthcare-cyberattack.html (last visited March 18, 2024).

[9] *See* https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm (last visited March 18, 2024)

the Company believes the network interruption is specific to Change Healthcare systems, and all other systems across the Company are operational."[10]

26. UHG initially claimed that a nation-state actor was responsible for the Data Breach. Blackcat, however, claimed responsibility for the Data Breach and stated on its dark web site that it had stolen the confidential health and personal identifying information relating to millions of Americans.

27. Specifically, Blackcat said it gained access to 6TB of data, including medical records, and payment and claims information containing personally identifiable information like names, contact information such as phone numbers and email addresses, and Social Security Numbers.

28. Blackcat also claimed to have stolen Change Healthcare's source code and the confidential and sensitive information of CVS Caremark, Metlife, Health Net, Federal Medicare, and Tricare.

29. Below is the statement that Blackcat issued regarding the cyberattack, indicating that the group has reviewed a substantial amount of confidential medical and personal identifying information:

> Change Healthcare - Optum - UnitedHealth
>
> 2/28/2024, 4:19:59 PM
>
> UnitedHealth has announced that the attack is "strictly related" to Change Healthcare only and it was initially attributed to a nation state actor.
>
> Two lies in one sentence.
>
> Only after threatning [sic] them to announce it was us, they started telling a different story.
>
> It is true that the attack is centered at Change Healthcare production and corporate networks, but why is the damage extremely high? Change Healthcare production servers process extremely sensitive data to all of UnitedHealth clients that rely on Change Healthcare technology solutions. Meaning thousands of healthcare providers, insurance providers, pharmacies, etc . . .

[10] *Id.*

Also, being inside a production network one can imagine the amount of critical and sensitive data that can be found.

We were able to exfiltrate to be exact more than 6 TB of highly selective data. The data relates to all Change Health clients that have sensitive data being processed by the company.

The list of affected Change Health partners that we have sensitive data for is actually huge with names such as:

- Medicare
- Tricare
- CVS-CareMark
- Loomis
- Davis Vision
- Health Net
- MetLife
- Teachers Health Trust
- Tens of insurance companies and others

Anyone with some decent critical thinking will understand what damage can be done with such intimate data on the affected clients of UnitedHealth/UnitedHealth solutions as well, beyond simple scamming/spamming.

After 8 days and Change Health have [sic] still not restored its operations and chose to play a very risky game hence our announcement today.

So for everyone, both those affected and fellow associates. [sic] to understand what is at stake our exfiltrated data includes millions of:

- active US military/navy personnel PII
- medical records
- dental records
- payments information
- Claims information
- Patients PII including Phone numbers/addresses/SSN/emails/etc ...
- 3000+ source code files for Change Health solutions (for source-code review gents out there)
- Insurance records
- many many more

> UnitedHealth you are walking on a very thin line be careful you just might fall over.
>
> PS: For all those cyber intelligence so called expert . . . we did not use ConnectWise exploit as our initial access so you should base your reports you tell people on actual facts not kiddi [sic] speculations.

30. Screenshots of some of the data were reportedly shared as proof of the Data Breach. On February 28, 2024, UHG confirmed that the Data Breach was perpetrated by Blackcat.

31. Blackcat has a reputation for engaging in "double extortion tactics," that is, exfiltrating confidential and sensitive data before using ransomware to encrypt the files.

32. On March 7, 2024, two weeks after the Data Breach, UHG said in a statement: "We are working aggressively on the restoration of our systems and services."[11] UHG also stated, "All of us at UnitedHealth Group feel a deep sense of responsibility for recovery and are working tirelessly to ensure that providers can care for their patients and run their practices, and that patients can get their medications. We're determined to make this right as fast as possible."[12]

33. Shortly after Defendants publicly announced the Data Breach, the AHA issued a security advisory notifying members and the public that "**Change Healthcare has not provided a specific timeframe for which recovery of the impacted applications is expected**" (emphasis in original).[13] The AHA also recognized that hospitals and health systems "may be experiencing challenges with obtaining care authorizations for their patients, as well as delays in payment."[14] It stated that it was in communication with the Department of Health and Human Services, including the Centers for Medicare & Medicaid Services, about "options to support patients' timely access

---

[11] *See* https://www.unitedhealthgroup.com/newsroom/2024/2024-03-07-uhg-update-change-healthcare-cyberattack.html (last visited March 18, 2024).

[12] *Id*.

[13] *See* https://www.aha.org/2024-02-24-update-unitedhealth-groups-change-healthcares-continued-cyberattack-impacting-health-care-providers (last visited March 18, 2024).

[14] *Id.*

to care and provide temporary financial support to providers. We also are having these discussions with Optum. We will provide more information as it becomes available."[15]

34. In a letter to Health and Human Services, the AHA stated that while the full scope was "unknown," the AHA expected impacts to be far-reaching given Change Healthcare's national presence.[16] The AHA also explained how the incident has affected healthcare providers in terms of being unable to collect revenue. "[W]ithout this critical revenue source, hospitals and health systems may be unable to pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission critical contract work in areas such as physical security, dietary and environmental services," the AHA stated.[17] "In addition, replacing previously electronic processes with manual processes will add considerable administrative costs on providers, as well as divert team members from other tasks. It is particularly concerning that while Change Healthcare's systems remain disconnected, it and its parent entities benefit financially, including by accruing interest on potentially billions of dollars that belong to health care providers."[18]

35. Antitrust experts have opined that the Data Breach shows why placing "one conglomerate at the center of multiple health care functions is inherently risky."[19]

//

[15] *Id.*

[16] *See* https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack (last visited March 18, 2024).

[17] *Id.*

[18] *Id.*

[19] *See* https://www.statnews.com/2024/02/27/change-healthcare-cyber-attack-reveals-consolidation-risks/ (last visited March 18, 2024).

C. The Data Breach and Shutdown have Created a National Crisis in the Healthcare Industry, Severely Impacting the Financial Security of Hundreds of Thousands of Healthcare Providers.

36. The Data Breach and resulting shutdown have had reverberations across the U.S. healthcare industry that continue today, and the fallout is placing healthcare providers in a precarious situation.

37. Since the discovery of the vulnerabilities in Defendants' computer networks on February 21, 2024, many healthcare providers have been unable to submit claims to insurers for payment, and many have not received payments for claims submitted before February 21, 2024. One physician, Dr. Purvi Parikh, told CNBC that her practice has not been paid by insurers for her patients' visits, which creates problems for paying operational expenses like medical supplies and payroll.[20] Dr. Parikh said there were no immediate workarounds and that it could take weeks to change to a new platform.[21]

38. Licensed clinical social worker Jenna Wolfson reported that she has been unable to receive any payments due to the Data Breach and that many of her colleagues are facing the same problems.[22] According to Wolfson, "There are people right now that might not see payment on the work that they're doing today for months, and they still have an entire practice to keep above water."[23]

39. Dr. Margaret Parsons, a dermatologist at a 20-person practice in Sacramento, California, told KFF Health News that she and her colleagues have not been able to electronically submit claims for payment since February 21, 2024 and that the payment process for California's

---

[20] *Id.*

[21] *Id.*

[22] *See* https://healthitsecurity.com/features/understanding-the-impact-of-the-change-healthcare-cyberattack-on-providers (last visited March 18, 2024).

[23] *Id.*

Medicare Program does not accept paper claims which usually take 3-6 months to process.[24] "We will be in trouble in very short order, and are very stressed," said Dr. Parsons.[25]

40. Dr. Stephen Sisselman, an independent primary care physician in New York, said, "How can you pay staff, supplies, malpractice insurance – all this – without revenue? It's impossible."[26]

41. If the shutdown lasts a month, Jackson Health Systems, in Miami-Dade Florida, will be short on as much as $30 million in payments, according to its chief revenue officer.[27]

42. According to the president of Florida Hospital Association, Mary Mayhew, her members built "sophisticated systems that are reliant on Change Healthcare,"[28] and that changing processes could take about 90 days during which they will have no cash flow. "It's not like flipping a switch," said Mayhew.[29]

43. On March 13, 2024, the AHA wrote to Senators Ron Wyden and Mike Crapo about the Data Breach. According to the AHA's letter, the downed systems "are hampering providers' ability to verify patients' health insurance coverage, process claims and receive payment from many payers, exchange clinical records with other providers, provide cost estimates and bill patients, and in some instances, access the clinical guidelines used in clinical decision support tools and as part of the prior authorization process."[30]

---

[24] *See* https://www.npr.org/sections/health-shots/2024/03/09/1237038928/health-industry-ransomware-cyberattack-change-healthcare-optum-uhc-united (last visited March 18, 2024).

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *See* https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack (last visited March 18, 2024).

44. Moreover, the AHA reported in its March 13th letter that in response to a recent AHA survey of hospitals with nearly 1,000 responses, "74% reported direct patient care impact, including delays in authorizations for medically necessary care."[31] Further, the AHA reported that:

> [H]ospitals, health systems and other providers are experiencing extraordinary reductions in cash flow, threatening their ability to make payroll and to acquire the medical supplies needed to provide care. In the same survey, 94% of hospitals reported that the Change Healthcare cyberattack was impacting them financially, with more than half reporting the impact as "significant or serious." Indeed, a third of the survey respondents indicated that the attack has disrupted more than half of their revenue. The urgency of this matter grows by the day.[32]

45. To make matters worse, on March 18, 2024, ratings agency Fitch said that certain healthcare providers that use its services may see a hit to their credit profile as a result of the Data Breach's impact on cash flows.[33]

D. The Data Breach and Resulting Shutdown were Foreseeable Risks of Which Defendants were on Notice and Could Have Prevented.

46. Cybercriminals target the healthcare industry the most due to the treasure trove of confidential health and personal information maintained and stored by healthcare organizations. In 2023, the FBI reported 249 ransomware attacks in the healthcare industry.[34] Cyberattacks have doubled from 2016 to 2021 and have resulted in the exposure of personal health information for approximately 42 million patients.[35]

47. The FBI warned healthcare stakeholders as early as 2014 that they are the target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems,

---

[31] *Id*.

[32] *See* https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack (last visited March 18, 2024).

[33] *See* https://www.reuters.com/business/healthcare-pharmaceuticals/fitch-says-unitedhealth-unit-hack-could-hit-smaller-pharmacies-care-providers-2024-03-18/ (last visited March 18, 2024).

[34] *See* https://www.npr.org/sections/health-shots/2024/03/09/1237038928/health-industry-ransomware-cyberattack-change-healthcare-optum-uhc-united (last visited March 18, 2024).

[35] *See* https://www.ncbi.nlm.nih.gov/pmc/articles (last visited March 18, 2024).

perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[36]

48. In 2017, the Department of Health and Human Services released a ransomware fact sheet making it clear to entities covered by the Health Insurance Portability and Accountability Act ("HIPAA") that "[w]hen electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule."[37]

49. Under the HIPAA Privacy Rules, a breach is defined as, "[t]he acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI."[38] Accordingly, a ransomware attack such as the one that occurred on February 21, 2024 is considered a breach under the HIPAA Rules because there was an access of PHI not permitted under the HIPAA Privacy Rule.

50. A ransomware attack is also considered a "Security Incident" under HIPAA. Under the HIPAA Rules, a "Security Incident" is defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." 45 CFR § 164.304. According to the Department of Health and Human Services, "[t]he presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule."[39]

---

[36] *See* https://publicintelligence.net/fbi-targeting-healthcare20(PII) (last visited March 18, 2024).

[37] *See* https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html (last visited March 18, 2024).

[38] *See* https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited March 18, 2024).

[39] *See* https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet (last visited March 18, 2024).

51. Data Breaches can be prevented. Approximately 80% of ransomware is delivered through email phishing attacks. Other means to deliver ransomware is through brute force attacks on open remote desktop protocol ports. To prevent ransomware attacks, organizations must provide training to its employees for the handling of suspicious emails. They can also disable macros, avoid storing passwords in plain text, and perform hunts and search for suspicious behavior in their networks, among other things.

52. This is not the first time that the UHG family has dealt with a data breach. In May 2023, United HealthCare, a UHG subsidiary, had to notify members that protective health information may have been compromised due to a credential stuffing attack that occurred on the United Healthcare mobile app in February 2023.[40]

53. Accordingly, Defendants knew, given the vast amount of PHI and PII that healthcare providers such as Plaintiffs and Class members acquire and transmit to Defendants directly or through vendors and that in turn, Defendants store and maintain, that they were a target for cybercriminals and should have taken all reasonable measures to avoid cyberattacks. Defendants also understood the risks posed by their insecure data security practices and computer networks. Defendants' failure to heed warnings and failure to adequately maintain their computer networks secure resulted in the shutdown and harm to Plaintiffs and Class members.

E. Defendants, at all Relevant Times, had a Duty to Plaintiffs and Class Members.

54. Defendants marketed their services to Plaintiffs and Class members, and were aware, at all relevant times, that healthcare providers such as Plaintiffs and Class members handle PHI and PII on a daily basis and that they are required by law to keep such data confidential. Thus, Defendants were required by law to properly secure their computer networks and encrypt and maintain PHI and PII using industry standard methods, utilize available technology to defend their computer networks from invasion, and act reasonably to prevent foreseeable harms.

[40] *See* https://www.hipaajournal.com/credential-stuffing-attack-exposed-united-healthcare-member-data/ (last visited March 18, 2024).

55. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between them, on the one hand, and Plaintiffs and the other Class members, on the other hand. The special relationship arose because Plaintiffs and the members of the Class entrusted Defendants (or their partners who entrusted Defendants) with PHI and PII. Defendants had the resources necessary to prevent the Data Breach and to protect their computer networks but neglected to adequately invest in security measures, despite their obligations to protect such information. Accordingly, Defendants breached their common law, statutory and other owed duties to Plaintiffs and Class members.

56. Defendants' duty to use reasonable security measures also arose under HIPAA. Defendants are covered by HIPAA and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. Under HIPAA, Defendants were required to "reasonably protect" PHI from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

57. Under HIPAA, Defendants were specifically required to do the following:

- Ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted. 45 C.F.R. § 164.306(a)(1);
- Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights. 45 C.F.R. § 164.312(a)(1);
- Implement adequate policies and procedures to prevent detect, contain, and correct security violations. 45 C.F.R. § 164.308(a)(1)(i);
- Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports. 45 C.F.R. § 164.308(a)(1)(ii)(D);

- Protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI. 45 C.F.R. § 164.306(a)(2);
- Protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information. 45 C.F.R. § 164.306(a)(3);
- Ensure compliance with HIPAA security standard rules by its workforces. 45 C.F.R. § 164.306(a)(4);
- Train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI. 45 C.F.R. § 164.530(b); and/or
- Render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as Defendants had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304 definition of encryption).

58. Defendants' duty to use reasonable security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities like Defendants.

59. The Data Breach and resulting shutdown of the Change Healthcare networks were a direct and proximate result of Defendants' failure to: (1) properly safeguard and protect computer networks with PHI and PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (2) establish and implement appropriate safeguards to ensure the security and confidentiality of PHI and PII; and (3) protect against reasonably foreseeable threats to the security or integrity of such information and computer networks.

F. Plaintiffs' Experiences

60. Plaintiff Therapy My Way ("TMW") is a licensed healthcare provider serving patients in Plainview, NY.

61. Plaintiff TMW (through its payroll account, DBA Psychological Assessment Screening Services), contracted with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

62. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Specifically, healthcare providers such as Plaintiff TMW submit their claims to Therapy Notes, which in turn uses Change Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff TMW.

63. Beginning on or around February 21, 2024, when Defendants' systems were shut down because of the Data Breach, Plaintiff TMW could no longer submit claims through Therapy Notes and obtain payments for those claims. Since the shutdown, Plaintiff TMW has not been paid for any claims despite continuing to treat patients. Plaintiff TMW relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to employees.

64. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff TMW has had to take out an emergency loan with an interest rate of 31% to meet payroll and pay other basic expenses. Plaintiff TMW's staff resources have also been diverted to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

65. Plaintiff Thomas Franco Therapy and Consulting ("Franco") is a licensed healthcare provider serving patients in Manhattan, New York; Arlington, Virginia; Jersey City, New Jersey; and Burlington, Vermont.

66. Plaintiff Franco contracted with Therapy Notes, which offers an integrated practice management system that provides healthcare providers with tools to streamline their operations.

67. Therapy Notes, in turn, partners with Change Healthcare to process insurance claims submitted by its clients, among other things. Specifically, healthcare providers such as

Plaintiff Franco submit their claims to Therapy Notes, which in turn uses Change Healthcare to process them with insurance and healthcare plans who then issue payments to providers, like Plaintiff Franco.

68. Beginning on or around February 21, 2024, when Defendants' systems were shut down because of the Data Breach, Plaintiff Franco could no longer submit claims through Therapy Notes and obtain payments for those claims. Since the shutdown, Plaintiff Franco has not been paid for any claims despite continuing to treat patients. Plaintiff Franco relies on the payments it receives from submitted claims to pay basic business expenses, including salaries and wages to himself and another employee.

69. As a result of Defendants' failure to maintain the security of their computer networks, Plaintiff Franco has had to take out a line of credit to meet payroll and pay other basic expenses. Plaintiff Franco's staff resources have also been diverted to trying to resolve the cash flow problems caused by the shutdown of Defendants' computer networks.

V. CLASS ACTION ALLEGATIONS

70. Plaintiffs bring this action individually and on behalf of all other persons similarly situated (the "Nationwide Class") pursuant to the Federal Rule of Civil Procedure 23(b)(2), (b)(3), and (c)(4).

71. The Nationwide Class is initially defined as follows:

> All healthcare providers in the United States whose use of Change Healthcare's services was disrupted by the Data Breach.

72. Additionally, pursuant to the Federal Rule of Civil Procedure 23(b)(2), (b)(3), and (c)(4), Plaintiffs bring this action on behalf of the following New York Class initially defined as:

> All healthcare providers in the state of New York whose use of Change Healthcare's services was disrupted by the Data Breach.

73. The Nationwide Class and the New York Class are referred to herein as "Class," unless otherwise stated.

74. Excluded from the proposed Class are Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well

as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members.

75. Plaintiffs reserve the right to re-define the Class definitions after conducting discovery.

76. **Numerosity (Fed. R. Civ. P. 23(a)(1))**. The Class members are so numerous that joinder of all members is impracticable. Based on information and belief, the Class includes over one million licensed healthcare providers. The parties will be able to identify the exact size of the Class through discovery and Defendants' records.

77. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2); 23(b)(3))**. Common questions of law and fact exist for each of the claims and predominate over questions affecting only individual members of the Class. Questions common to the Class include, but are not limited to, the following:

a. Whether Defendants owed Plaintiffs and Class members a legal duty to implement and maintain reasonable security procedures and practices to protect PHI and PII;

b. Whether Defendants breached their legal duties to Plaintiffs and Class members;

c. Whether Defendants were negligent;

d. Whether Plaintiffs and Class members conferred benefits on Defendants;

e. Whether Defendants were unjustly enriched; and

f. Whether Plaintiff and Class members are entitled to relief, including damages and equitable relief.

78. **Typicality (Fed. R. Civ. P. 23(a)(3))**. Pursuant to Rule 23(a)(3), Plaintiffs' claims are typical of the claims of the Class members. Plaintiffs, like all Class members, suffered harm as a result of the Data Breach and ensuing shutdown of Defendants' computer networks.

79. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4))**. Pursuant to Rule 23(a)(4), Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Plaintiffs have no interest antagonistic to, or in conflict with, the interests of the Class members. Plaintiffs have retained counsel experienced in prosecuting class actions and data breach cases.

80. **Superiority (Fed. R. Civ. P. 23(b)(3))**. Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual Class members because the amount of monetary relief available to individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

81. **Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)).** In the alternative, this action may properly be maintained as a class action, because:

a. the prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual Class members which would establish incompatible standards of conduct for Defendants; or

b. the prosecution of separate actions by individual Class members would create a risk of adjudications with respect to individual Class members which would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

c. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

82. **Issue Certification (Fed. R. Civ. P. 23(c)(4))**. In the alternative, the common questions of fact and law, set forth in Paragraph 77, are appropriate for issue certification on behalf of the proposed Class.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

83. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

84. Defendants had (and continue to have) a legal duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting confidential health and personal identifying information on their network systems provided to them by Plaintiffs and Class members. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated.

85. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between them and Plaintiffs and Class members, which is recognized by state and federal law, including but not limited to HIPAA. Only Defendants, however, were in a position to ensure that their computer networks were sufficient to protect against the harm to Plaintiffs and the Class members that resulted from the Data Breach and ensuing shutdown. Plaintiffs relied on Defendants to implement and maintain reasonable security security procedures and practices to protect PHI and PII, and Defendants were aware of Plaintiffs' reliance.

86. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting PHI and PII on their network systems by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PHI and PII entrusted to them. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting PHI and PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in harm to Plaintiffs and Class members.

87. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached their duties to Plaintiffs and Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting their data networks and PHI and PII within their possession, custody, and control, which resulted in the shutdown of Defendants' computer networks and disrupted Plaintiffs' and Class members' businesses.

88. Defendants, by and through their negligent actions, inactions, omissions, and want of ordinary care, further breached their duties to Plaintiffs and Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting PHI and PII received from Plaintiffs and Class members.

89. But for Defendants' negligent breach of the above-described duties owed to Plaintiffs and Class members, Defendants would not have experienced the Data Breach and would not have had to shut down the Change Healthcare networks, thereby preventing Plaintiffs and Class members from (i) timely receiving payments for previously submitted claims, (ii) submitting new claims for payment, and (iii) obtaining insurance authorization for patient medical treatment, among other things. The harms to Plaintiffs and Class members were foreseeable given the types of services Defendants provide healthcare providers such as Plaintiffs and Class members and the statutory obligations shared by all to protect computer networks and confidential PHI and PII.

90. Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and directly resulted in the shutdown of the Change Healthcare computer networks constitute negligence.

91. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and the related shutdown, Plaintiffs and Class members have suffered (and will continue to suffer) monetary losses and economic harms and seek all available damages.

COUNT II
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class)

92. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

93. Plaintiffs and Class members conferred benefits on Defendants in the form of payments for claims management and processing, insurance verification, authorization and medical necessity reviews, and disbursement of payments, among other things, both directly and indirectly. Defendants had knowledge of the benefits conferred by Plaintiffs and Class members and appreciated such benefits. Defendants should have used, in part, the monies Plaintiffs and Class members paid to them, directly and indirectly, to pay the costs of reasonable data privacy and security practices and procedures.

94. Plaintiffs and Class members have suffered actual damages and harm as a result of Defendants' conduct, inactions, and omissions. Defendants should be required to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds received from Plaintiffs and Class members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the members of the Class defined above, respectfully request that this Court enter:

(a) An order certifying this case as a class action under Federal Rule of Civil Procedure 23, appointing Plaintiffs as the Class representatives, and appointing the undersigned as Class counsel;

(b) A judgment awarding Plaintiffs and Class members appropriate monetary relief, including damages, equitable relief, restitution, and disgorgement;

(c) An order entering injunctive and declaratory relief as appropriate under the applicable law;

(d) An order awarding Plaintiffs and the Class pre-judgment and/or post-judgment interest as prescribed by law;

(e) An order awarding reasonable attorneys' fees and costs as permitted by law; and

(f) Any and all other and further relief as may be just and proper.

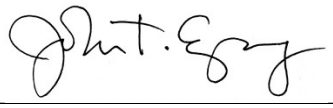
//

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial.

Dated: March 26, 2024

SPRAGENS LAW PLC



John T. Spragens (TN No. 31445)
311 22nd Ave. N.
Nashville, TN 37203
Telephone: (615) 983-8900
Facsimile: (615) 682-8533
john@spragenslaw.com

GIBBS LAW GROUP LLP
Rosemary M. Rivas
David M. Berger
Rosanne L. Mah
1111 Broadway, Suite 2100
Oakland, California 94607
(510) 350-9700 (tel.)
(510) 350-9701 (fax)
rmr@classlawgroup.com
dmb@classlawgroup.com
rlm@classlawgroup.com

Attorneys for Plaintiffs